

# Consegna:

L'esercizio di oggi mira a consolidare le conoscenze acquisite.

Vedremo due esercizi: I) la configurazione di una policy sul firewall windows; II) una packet capture con Wireshark.

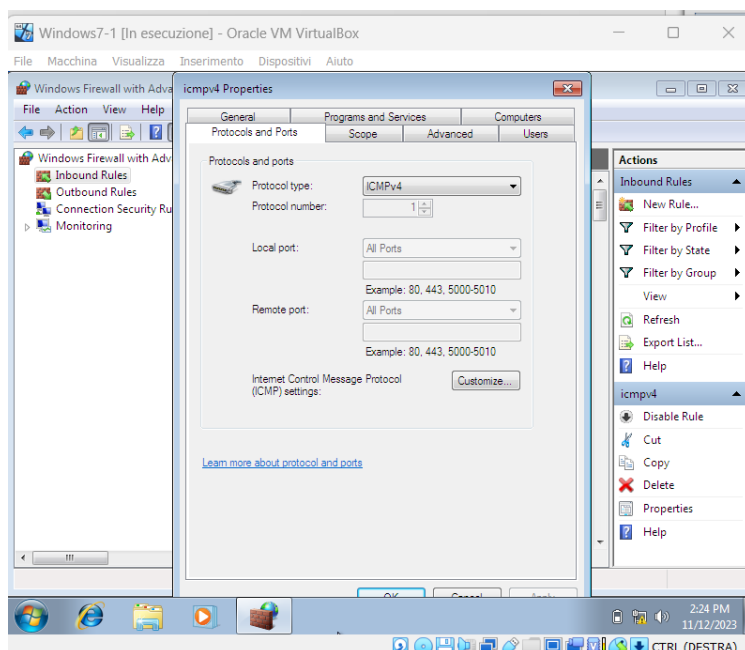
Vedremo anche come simulare alcuni servizi di rete con un tool pre-installato su Kali Linux (InetSim)

## Esercizio:

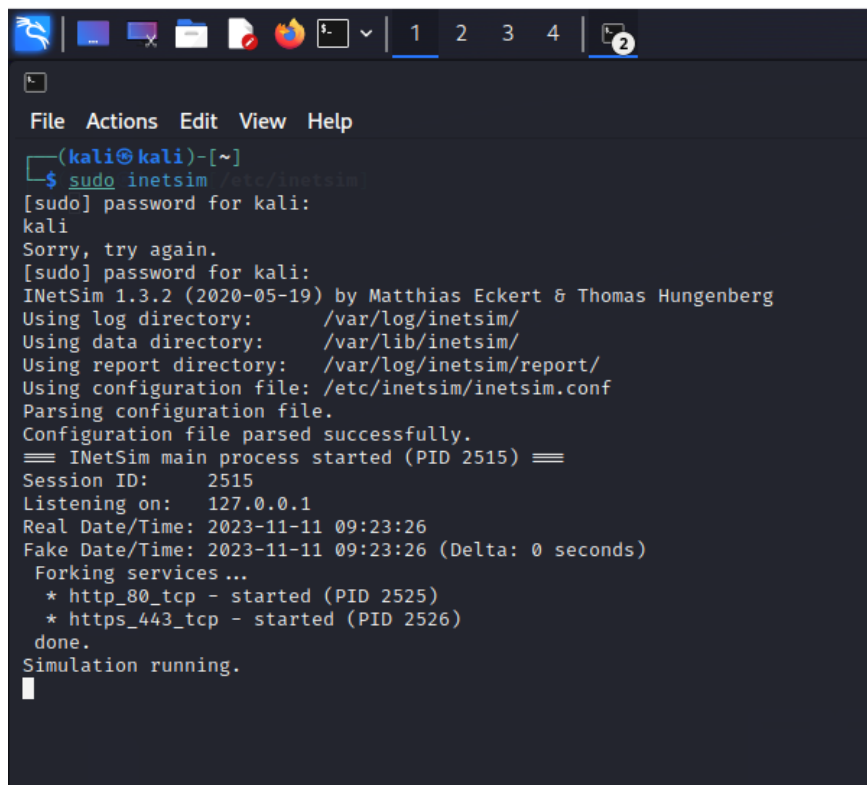
- ❑ Configurare policy per permettere il ping da macchine Linux a Macchina Windows 7 nel nostro laboratorio (Windows firewall)
- ❑ Utilizzo dell'utility InetSim per l'emulazione di servizi Internet
- ❑ Cattura di pacchetti con Wireshark

# Soluzione:

**Punto 1:** Ho configurato la policy di Windows 7 abilitando tutti i Firewall e creando 2 nuove regole con la finalità di consentire la comunicazione tra i sistemi operativi (Linux e Win7); nel fare ciò sono andata sulle impostazioni avanzate del Firewall e creato nuove regole in entrata in uscita con la finalità di consentire il ping tra le varie macchine virtuali.

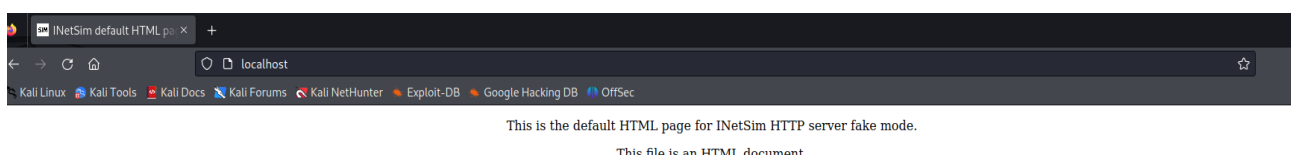


**Punto 2:** Ho eseguito la configurazione dell'utility InetSim all'interno del laboratorio virtuale di kali Linux, nel fare ciò ho eseguito dal terminale di Linux il comando `cd/etc/inetSim`, una volta entrata nella directory ho lanciato il comando `'ls'` ed ho aperto il file `'inetSim.conf'` tramite il comando `'nano inetSim.conf'`, una volta aperto il file ho disabilitato tutti i servizi fatta eccezione del servizio `http` ed `https`, dopodichè ho cambiato il service bind address da `10.10.10.1` a `127.0.0.1`. Fatto tutto ciò ho salvato la configurazione e fatto partire l'utility tramite il comando `'sudo inetSim'`.



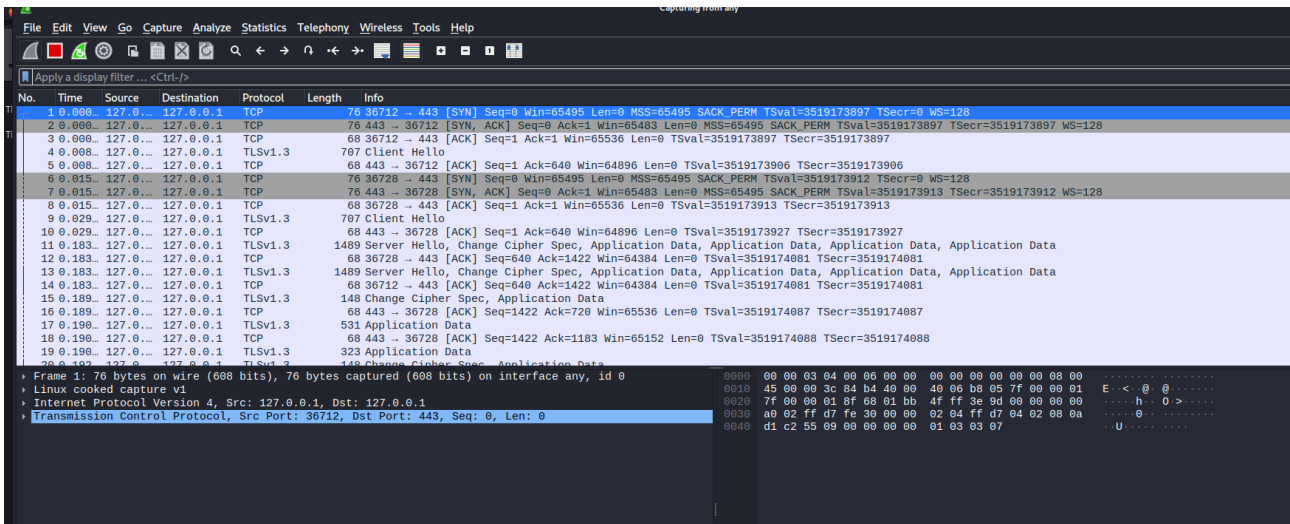
```
(kali㉿kali)-[~]
└─$ sudo inetSim /etc/inetSim
[sudo] password for kali:
kali
Sorry, try again.
[sudo] password for kali:
INetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg
Using log directory: /var/log/inetSim/
Using data directory: /var/lib/inetSim/
Using report directory: /var/log/inetSim/report/
Using configuration file: /etc/inetSim/inetSim.conf
Parsing configuration file.
Configuration file parsed successfully.
=== INetSim main process started (PID 2515) ===
Session ID: 2515
Listening on: 127.0.0.1
Real Date/Time: 2023-11-11 09:23:26
Fake Date/Time: 2023-11-11 09:23:26 (Delta: 0 seconds)
Forking services...
* http_80_tcp - started (PID 2525)
* https_443_tcp - started (PID 2526)
done.
Simulation running.
```

Dopodichè ho aperto il browser e cercato `'https://localhost/'` e `'http://localhost.sample.txt'`



**Punto 3:** Ho aperto da Linux l'applicazione Wireshark mentre avevo aperte le 2 pagine nel browser viste poc'anzi. Una volta aperta la schermata di WS ho aperto 'any' e da qui ho riscontrato quanto segue.

PS. Cercando sul browser 'http://localhost/sample.txt su wireshark ho riscontrato questo traffico:



Invece cercando sul browser 'http://localhost/' ho riscontrato questo traffico:

